PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-242604
(43)Date of publication of application : 08.09.2000

(51)Int.Cl. G06F 15/00
G06F 9/06
G06F 12/14
G06F 13/00
G06F 17/60

(21)Application number : 11-042197
(22)Date of filing : 19.02.1999

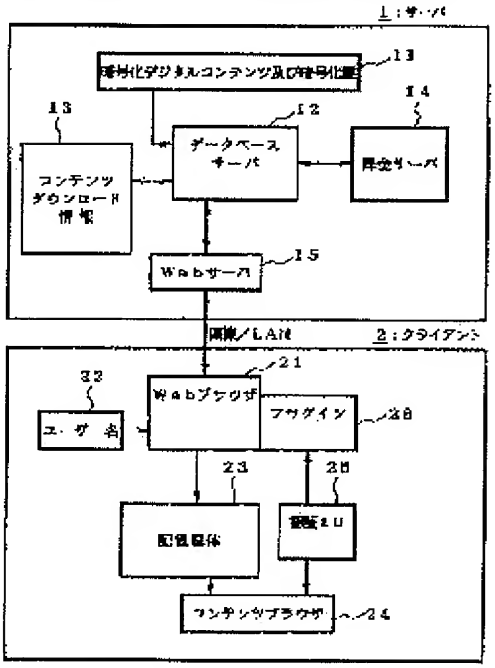
(71)Applicant : FUJITSU LTD
(72)Inventor : HARAKI TAKASUKE

(54) CONTENTS DISTRIBUTION SYSTEM, TERMINAL DEVICE AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the unauthorized use of contents and to provide the appro priate use of the contents by giving no permission or performing recharging for a re-downloading request from different terminals by the same user with respect to the contents distribution system, terminal equipment and a recording medium.

SOLUTION: This system is provided with a means for receiving a user ID, the unique authentication ID of the terminal and the downloading request of the contents, a table for registering the user ID, the authentication ID and transmitted contents in correspondence to each other, the means for generating a decoding key from the authentication ID and the key of the contents when the received user ID and the contents are registered in the table and the received authentication ID is the same or registering the user ID, the authentication ID and the contents in the table in correspondence to each other and generating the decoding key from the authentication ID and the key of the contents when the user ID and the contents are not registered in the table and the means for transmitting the generated decoding key and ciphered contents to the terminal.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－242604
（P2000－242604A）
(43)公開日　平成12年９月８日(2000.9.8)

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
G06F 15/00	310	G06F 15/00	310A	5B017
9/06	550	9/06	550C	5B049
			550Z	5B076
12/14	320	12/14	320F	5B085
13/00	354	13/00	354Z	5B089

審査請求　未請求　請求項の数７　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平11－42197

(22)出願日　平成11年２月19日(1999.2.19)

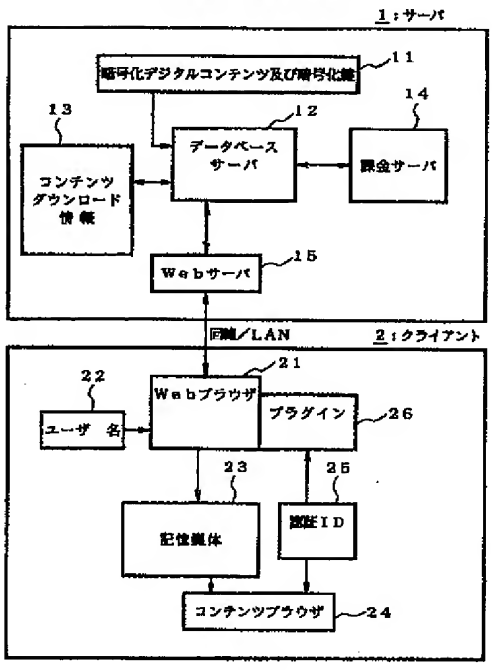
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　原木　貴祐
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100089141
弁理士　岡田　守弘

最終頁に続く

(54)【発明の名称】　コンテンツ配布システム、端末装置および記録媒体

(57)【要約】
【課題】　本発明は、コンテンツ配布システム、端末装置および記録媒体に関し、同一ユーザによる異なる端末からの再ダウンロード要求に対して不許可あるいは再課金などし、コンテンツの無断使用を防止すると共にコンテンツの適切な使用を実現することを目的とする。
【解決手段】　ユーザＩＤ、端末の一意の認証ＩＤおよびコンテンツのダウンロード要求を受信する手段と、ユーザＩＤ、認証ＩＤおよび送信したコンテンツを対応づけて登録するテーブルと、受信したユーザＩＤとコンテンツがテーブルに登録されており、かつ受信した認証ＩＤが同一であったときには認証ＩＤとコンテンツの鍵とから解読鍵を生成、あるいはユーザＩＤとコンテンツがテーブルに登録されていなかったときにはテーブルにユーザＩＤ、認証ＩＤ、コンテンツを対応づけて登録すると共に認証ＩＤとコンテンツの鍵とから解読鍵を生成する手段と、生成した解読鍵および暗号化したコンテンツを端末に送信する手段とを備えるように構成する。

本発明のシステム構成図



【特許請求の範囲】

【請求項１】コンテンツを配布するシステムにおいて、ユーザＩＤ、端末の一意の認証ＩＤおよびコンテンツのダウンロード要求を受信する手段と、

ユーザＩＤ、認証ＩＤおよび送信したコンテンツを対応づけて登録するテーブルと、

上記受信したユーザＩＤとコンテンツが上記テーブルに登録されており、かつ受信した認証ＩＤが同一であったときには認証ＩＤとコンテンツの鍵とから解読鍵を生成、あるいはユーザＩＤとコンテンツが上記テーブルに登録されていなかったときには上記テーブルにユーザＩＤ、認証ＩＤ、コンテンツを対応づけて登録すると共に認証ＩＤとコンテンツの鍵とから解読鍵を生成する手段と、

上記生成した解読鍵および上記暗号化したコンテンツを上記端末に送信する手段とを備えたことを特徴とするコンテンツ配布システム。

【請求項２】上記受信したユーザＩＤとコンテンツが上記テーブルに登録されており、かつ受信した認証ＩＤが同一でなかったときに、上記端末に再課金の旨を送信し、当該端末から再課金の了解の旨の応答があったときには、認証ＩＤとコンテンツの鍵とから解読鍵を生成し、生成した解読鍵および暗号化したコンテンツを端末に送信することを特徴とする請求項１記載のコンテンツ配布システム。

【請求項３】上記受信したユーザＩＤとコンテンツが上記テーブルに登録されており、かつ受信した認証ＩＤが異なるときには、再課金を行うと共に、認証ＩＤとコンテンツの鍵とから解読鍵を生成し、生成した解読鍵および鍵で暗号化したコンテンツを端末に送信することを特徴とする請求項１記載のコンテンツ配布システム。

【請求項４】上記受信したユーザＩＤとコンテンツが上記テーブルに登録されており、かつ受信した認証ＩＤが異なるときには、上記受信した認証ＩＤと上記テーブルに登録されているコンテンツの鍵とから１の解読鍵を生成、および当該受信した認証ＩＤとダウンロード要求のあった現在のコンテンツの鍵とから２の解読鍵を生成し、生成した１の解読鍵と暗号化したコンテンツおよび生成した２の解読鍵と暗号化したコンテンツの両者を端末に送信することを特徴とする請求項１記載のコンテンツ配布システム。

【請求項５】ユーザＩＤ、自身の一意の認証ＩＤ、およびコンテンツのダウンロード要求を送信する手段と、

送信されてきた解読鍵およびコンテンツを受信する手段と、

上記受信した解読鍵について、自身の所定の認証ＩＤをもとにコンテンツの鍵を生成する手段と、

上記生成した鍵をもとに、上記受信した暗号化されたコンテンツを復号する手段と、

上記復号されたコンテンツを使用する手段とを備えたことを特徴とする端末装置。

【請求項６】上記端末の一意の認証ＩＤを、上記端末の所定のハードウェアの一意の番号としたことを特徴とする請求項５記載の端末。

【請求項７】ユーザＩＤ、端末の一意の認証ＩＤおよびコンテンツのダウンロード要求を受信する手段と、

ユーザＩＤ、認証ＩＤおよび送信したコンテンツを対応づけてテーブルに登録する手段と、

上記受信したユーザＩＤとコンテンツが上記テーブルに登録されており、かつ受信した認証ＩＤが同一であったときには認証ＩＤとコンテンツの鍵とから解読鍵を生成、あるいはユーザＩＤとコンテンツが上記テーブルに登録されていなかったときには上記テーブルにユーザＩＤ、認証ＩＤ、コンテンツを対応づけて登録すると共に認証ＩＤとコンテンツの鍵とから解読鍵を生成する手段と、

上記生成した解読鍵および上記暗号化したコンテンツを上記端末に送信する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツを配布および配布されたコンテンツを使用するコンテンツ配布システム、端末装置および記録媒体に関するものである。

【０００２】

【従来の技術】近年、音楽や映画、更にＴＶゲームなどのプログラムのデジタルのコンテンツは通信の普及により、店頭で購入するでけでなく、オンラインで購入することが可能となとっている。特に、インターネットによるWWWサーバの出現により、ユーザはWWWサーバに接続してコンテンツ一覧をダウンロードしてクライアントの画面上に表示し、視覚的に見てから選択して購入することが可能となっている。

【０００３】この際、デジタルのコンテンツという性質上、コンテンツをコピーしても劣化しないので、コピーが無限に繰り返されてしまい、コンテンツの著作者の保護が行えない。そのため、ユーザがインターネットなどのネットワークを介して正規に購入したコンテンツについて、他人の無断使用を防止することが要望されている。

【０００４】

【発明が解決しようとする課題】このため、例えばユーザがネットワークを介してWWWサーバからコンテンツを正規に購入してダウンロードしハードディスク装置に格納して使用しようとする場合、ダウンロード中に何らかの障害でダウンロードに失敗し、再度ダウンロードをしようとしたときに、WWWサーバ側で正規購入したユーザＩＤを記憶しておき当該再度のダウンロード要求のあったユーザＩＤが記憶されていたときに再ダウンロー

ドを許可するようにすると、他のパソコンからユーザＩＤを指定した再ダウンロード要求があると許可されてしまい、ユーザＩＤが盗用されるとコンテンツが不当にＷＷＷサーバから第三者にダウンロードされていしまうなどの問題がある。このため、コンテンツの無断使用を防止すると共に異なるパソコンなどからの再ダウンロード要求時に適切な使用を許可することが望まれている。

【０００５】本発明は、これらの問題を解決するため、同一ユーザによる異なる端末からの再ダウンロード要求に対して不許可あるいは再課金などし、コンテンツの無断使用を防止すると共にコンテンツの適切な使用を実現することを目的としている。

【０００６】

【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、サーバ１は、ユーザＩＤ、端末の一意の認証ＩＤおよびコンテンツのダウンロード要求を受信したり、認証ＩＤとコンテンツの鍵とから解読鍵を生成したり、生成した解読鍵および暗号化したコンテンツを端末に送信したりなどするものである。

【０００７】クライアント２は、ユーザＩＤ、自身の一意の認証ＩＤ、およびコンテンツのダウンロード要求を送信したり、送信されてきた解読鍵およびコンテンツを受信したり、受信した解読鍵について自身の所定の認証ＩＤをもとにコンテンツの鍵を生成したり、生成した鍵をもとに暗号化されたコンテンツを復号したりなどするものである。

【０００８】次に、動作を説明する。サーバ１がユーザＩＤ、端末の一意の認証ＩＤおよびコンテンツのダウンロード要求を受信し、受信したユーザＩＤとコンテンツがコンテンツテーブルに登録されており、かつ受信した認証ＩＤが同一であったときには認証ＩＤとコンテンツの鍵とから解読鍵を生成、あるいはユーザＩＤとコンテンツがコンテンツテーブルに登録されていなかったときには上記テーブルにユーザＩＤ、認証ＩＤ、コンテンツを対応づけて登録すると共に認証ＩＤとコンテンツの鍵とから解読鍵を生成し、生成した解読鍵および暗号化したコンテンツを端末に送信するようにしている。

【０００９】この際、受信したユーザＩＤとコンテンツがコンテンツテーブルに登録されており、かつ受信した認証ＩＤが同一でなかったときに、端末に再課金の旨を送信し、端末から再課金の了解の旨の応答があったときには、認証ＩＤとコンテンツの鍵とから解読鍵を生成し、生成した解読鍵および暗号化したコンテンツを端末に送信するようにしている。

【００１０】また、受信したユーザＩＤとコンテンツがコンテンツテーブルに登録されており、かつ受信した認証ＩＤが異なるときには、再課金を行うと共に、認証ＩＤとコンテンツの鍵とから解読鍵を生成し、生成した解読鍵および暗号化したコンテンツを端末に送信するようにしている。

【００１１】また、受信したユーザＩＤとコンテンツがコンテンツテーブルに登録されており、かつ受信した認証ＩＤが異なるときには、受信した認証ＩＤとコンテンツテーブルに登録されているコンテンツの鍵とから１の解読鍵を生成、および受信した認証ＩＤとダウンロード要求のあった現在のコンテンツの鍵とから２の解読鍵を生成し、生成した１の解読鍵と暗号化したコンテンツおよび生成した２の解読鍵と暗号化したコンテンツの両者を端末に送信するようにしている。

【００１２】また、クライアント（端末）２）がユーザＩＤ、自身の一意の認証ＩＤ、およびコンテンツのダウンロード要求を送信し、送信されてきた解読鍵およびコンテンツを受信し、受信した解読鍵について自身の所定の認証ＩＤをもとにコンテンツの鍵を生成し、生成した鍵をもとに受信した暗号化されたコンテンツを復号し、復号したコンテンツを使用するようにしている。

【００１３】また、クライアント（端末）２の一意の認証ＩＤを、クライアント（端末）２の所定のハードウェアの一意の番号とするようにしている。従って、同一ユーザによる異なるクライアント（端末）２からの再ダウンロード要求に対して不許可あるいは再課金などすることにより、コンテンツの無断使用を防止すると共にコンテンツの適切な使用を実現することが可能となる。

【００１４】

【実施例】次に、図１から図６を用いて本発明の実施の形態および動作を順次詳細に説明する。

【００１５】図１は、本発明のシステム構成図を示す。図１において、サーバ１は、デジタルのコンテンツを複数のクライアント２に配布（ダウンロード）するものであって、ここでは、図示の１１ないし１５などから構成されるものである。

【００１６】暗号化デジタルコンテンツ及び暗号化鍵１１は、ユーザに配布する暗号化したデジタルのコンテンツと、その暗号化鍵（デジタルコンテンツを暗号化したり、暗号化したデジタルコンテンツを解読する鍵）であって、データベースに保存したものである。

【００１７】データベースサーバ１２は、暗号化デジタルコンテンツ及び暗号鍵１１を保存したデータベースを管理するサーバであって、ここでは、ユーザからダウンロード要求のあったコンテンツとその鍵（解読鍵）を読み出してＷｅｂサーバ１５にわたしたり、ダウンロードさせたコンテンツとそのユーザＩＤなどを課金サーバ１４に通知して課金したりなどするものである。

【００１８】コンテンツダウンロード情報１３は、ユーザからダウンロード要求のあったコンテンツダウンロード情報を保存したものであって、後述する図３の（ａ），（ｂ）のユーザ認証テーブルおよびコンテンツテーブルなどをもとにユーザにダウンロードしたコンテンツを管理するためのものである。

【００１９】課金サーバ１４は、ユーザにダウンロードしたコンテンツの使用料をユーザ毎に管理し、所定期間毎に集計して各ユーザに請求したりなどするものである。Ｗｅｂサーバ１５は、クライアント２から回線やＬＡＮなどを介して接続し、コンテンツ一覧を送信したり、コンテンツ一覧から選択したコンテンツのダウンロード要求を受け付けたり、要求のあったコンテンツをダウンロードしたりなどするものである。

【００２０】クライアント２は、ユーザが使用する端末（パソコン）などであって、回線やＬＡＮなどを介してＷｅｂサーバ１５に接続し、コンテンツ一覧をダウンロードして表示し、表示させたコンテンツ一覧上で選択したコンテンツのダウンロード要求したり、ダウンロードされてきたコンテンツを記憶媒体２３に格納して鍵で暗号化されたコンテンツを復号してしようしたりなどするものであって、２１ないし２６などから構成されるものである。

【００２１】Ｗｅｂブラウザ２１は、回線やＬＡＮなどを介してＷｅｂサーバ１５に接続して、コンテンツ一覧をダウンロードして表示したりなどするものである。ユーザ名２２は、クライアント（端末）２を操作してコンテンツを使用（コンテンツを試聴、表示などして使用）するユーザ名（ユーザの氏名、ユーザＩＤなどの情報）である。

【００２２】記憶媒体２３は、Ｗｅｂサーバ１５からダウンロードしたコンテンツを格納する記憶媒体であって、例えばハードディスク装置、ＤＶＤ－ＲＡＭなどの記憶媒体である。

【００２３】コンテンツブラウザ２４は、記憶媒体２３に記憶させた暗号化されたコンテンツを、クライアント２のハードウェアが持つ一意の認証ＩＤ（例えばハードディスク装置の番号）２５と解読鍵（コンテンツのダウンロード時に一緒にＷｅｂサーバ１５からダウンロードされた解読鍵、図２参照）をもとに復号した鍵で、復号して使用（例えば音楽のときは試聴、ＴＶゲームのプログラムの場合にはその復号したプログラムで遊戯など）するものである。

【００２４】認証ＩＤ２５は、クライアント（端末）２に一意のＩＤであって、例えばハードウェアであるハードディスク装置の番号である。プラグイン２６は、Ｗｅｂブラウザ２１に組み込む各種機能を持ったソフトウエアであって、ここでは、クライアント（端末）２のハードウェアの一意の認証ＩＤ２６を取り出して、コンテンツ要求と一緒にしてＷｅｂサーバ１５に送信したり等するものである（図２など参照）。

【００２５】次に、図２のフローチャートの順番に従い、図１の構成の動作を詳細に説明する。図２は、本発明の動作説明フローチャート（その１）を示す。ここで、サーバ１およびクライアント２は図１のサーバ１およびクライアント２に相当する。

【００２６】図２において、Ｓ１は、コンテンツ一覧の表示要求を行う。これは、図１のクライアント２を構成するＷｅｂブラウザ２１上に表示した例えばホームページの画面上でコンテンツ一覧を選択して要求する。

【００２７】Ｓ２は、コンテンツ一覧を返信する。これは、Ｓ１のコンテンツ一覧要求に対応して、Ｗｅｂサーバ１５がコンテンツ一覧を返信する。Ｓ３は、コンテンツ表示・選択する。これは、Ｓ２で返信されたコンテンツ一覧をＷｅｂブラウザ２１の画面上に表示し、ユーザがコンテンツ一覧からコンテンツを１つマウスなでクリックして選択する。

【００２８】Ｓ４は、ユーザＩＤ（ＵＩＤ）を入力する。Ｓ５は、認証ＩＤ（ＭＩＤ）を取得する。これらＳ４、Ｓ５はＷｅｂブラウザ２１がユーザＩＤを取り込むと共に、プラグイン２６を構成するソフトウエアに指示して認証ＩＤ（例えばハードディスク装置の番号）を取り込む。そして、これらユーザＩＤおよび認証ＩＤをＷｅｂサーバ１５に送信する。

【００２９】Ｓ６は、ユーザＩＤをチェックする。これは、Ｓ４で送信されてきたユーザＩＤが後述する図３の（ａ）のユーザ認証テーブル３１に登録されており、コンテンツをダウンロードする資格があるかチェックする。この際、合わせてユーザのパスーワードも一致するかチェックする。チェックした結果、ＯＫとなった場合には、Ｓ７に進む。ＮＧの場合には、エラー処理を行う。

【００３０】Ｓ７は、コンテンツテーブルの認証ＩＤと同じか判別する。これは、後述する図３の（ｂ）のコンテンツテーブル３２を参照し、Ｓ４、Ｓ５でダウンロード要求のあったユーザＩＤとコンテンツＩＤに一致するエントリがあり、当該エントリ中の認証ＩＤに今回の送信されてきた認証ＩＤが一致するか判別する。一致する場合には、今回のダウンロード要求のあった

・コンテンツＩＤ：
・ユーザＩＤ　　：
・認証ＩＤ　　：

の３つが一致する図３の（ｂ）のコンテンツテーブル３２中のエントリがあり、過去に同一のパソコン（クライアント２）がコンテンツをダウンロードを受けていると判明して既にコンテンツの使用許諾を与えたユーザに対する２回目（あるいは２回目以降）のダウンロードと判明（例えばダウンロード途中に何らかの原因によってダウンロード失敗して２回目の再ダウンロード要求と判明）したので、Ｓ８に進む。尚、図示しないが今回のダウンロード要求のあった

・コンテンツＩＤ：
・ユーザＩＤ　　：
・認証ＩＤ　　：

中のユーザＩＤとコンテンツＩＤとが図３の（ｂ）のコンテンツテーブル３２に設定されていないときは、当該

ユーザが始めて当該コンテンツのダウンロードを要求したと判明するので、初回の処理として、コンテンツテーブル３２に、コンテンツＩＤ、ユーザＩＤ、認証ＩＤを設定した後、Ｓ８に進む。

【００３１】Ｓ８は、認証ＩＤ＋鍵をもとに解読鍵を作成する。これは、クライアント２から受信した認証ＩＤと、ダウンロード要求したコンテンツの鍵とをもとに解読鍵を作成（例えば認証ＩＤを鍵で暗号化して解読鍵を作成）する。

【００３２】Ｓ９は、コンテンツ＋解読鍵を送信する。これにより、サーバ１は、暗号化したコンテンツと、Ｓ８で作成した解読鍵とをクライアント２に送信できたこととなる。

【００３３】Ｓ１０は、コンテンツデータベースの例を示す。ここでは、暗号化したコンテンツと鍵とからコンテンツが構成される様子を示す。このコンテンツの鍵を、既述したＳ８の鍵とし、認証ＩＤを当該鍵で暗号化して解読鍵を作成する。

【００３４】Ｓ１１は、クライアント２がＳ９でサーバ２から送信された、暗号化されたコンテンツと解読鍵を受信する。Ｓ１２は、コンテンツを保存・解読鍵を保存する。

【００３５】Ｓ１３は、ブラウザ起動する。これは、図１のコンテンツブラウザ２４を起動する。Ｓ１４は、コンテンツを読み込む。

【００３６】Ｓ１５は、解読鍵を読み込む。これらＳ１４、Ｓ１５は、Ｓ１２で保存した暗号化したコンテンツおよび解読鍵をコンテンツブラウザ２４が読み込む。Ｓ１６は、認証ＩＤを取得する。これは、コンテンツブラウザ２４が、クライアント（パソコンなど）２の予め決めたハード装置の固有の一意の番号例えばハードディスク装置の一意の番号を認証ＩＤとして取得する。

【００３７】Ｓ１７は、鍵を再生する。これは、Ｓ１４からＳ１６で読込みおよび取得した、解読鍵を認証ＩＤで復号して鍵（暗号化されているコンテンツを復号する鍵）を再生する。

【００３８】Ｓ１８は、正しい鍵か判別する。これは、Ｓ１７で再生した鍵が正しいか判別する．ＹＥＳの場合には、Ｓ１９に進む。ＮＯの場合には、Ｓ２１でエラーメッセージを表示、例えば図示のように

・異なる認証ＩＤのマシンです。このマシンではこのコンテンツは使用出来ません。というメッセージを表示して終了する。

【００３９】Ｓ１９は、コンテンツ復号する。これは、ダウンロードした暗号化されたコンテンツを鍵で復号して元のコンテンツにする。Ｓ２０は、コンテンツ使用する。これは、Ｓ１９で復号したコンテンツを使用、例えば音楽の場合には試聴し、ＴＶゲームのプログラムの場合には動作させてＴＶゲームを楽しみ、各種有用情報の場合にはその情報を読んだり使用して業務を行ったりなどの使用を行う。

【００４０】以上によって、クライアント２がコンテンツＩＤ、ユーザＩＤ、認証ＩＤをサーバ１に送信し、サーバ１が認証ＩＤと鍵から解読鍵を作成して暗号化したコンテンツと一緒にクライアント２に送信し、これら解読鍵と暗号化したコンテンツを受信したクライアント２が自身の固有の認証ＩＤをもとに解読鍵から鍵を復号し、復号した鍵で暗号化されたコンテンツを復号して元のコンテンツを生成し、この生成したコンテンツを使用することが可能となる。これにより、同一ユーザであっても、異なるクライアント（異なるマシン）では暗号化されたコンテンツを復号できず、無断使用を防止することが可能となると共に、同一のクライアント（同一のマシン）から再ダウンロードを受けてコンテンツを復号して使用することが可能となる。

【００４１】図３は、本発明のテーブル例を示す。図３の（ａ）は、サーバ１側で管理するユーザ認証テーブル３１の例を示す。このユーザ認証テーブル３１は、図１のサーバ１側に用意し、コンテンツの使用を許可して課金する対象のユーザＩＤとパスワードを対応づけて予め登録する。このユーザ認証テーブル３１を設けて、既述した図２のＳ６のときに参照して、ユーザＩＤとパスワードとを確認し、登録されているときにＯＫ（ユーザ認証ＯＫ）と判定する。

【００４２】図３の（ｂ）は、サーバ１側で管理するコンテンツテーブル３２の例を示す。このコンテンツテーブル３２は、図１のサーバ１側に用意し、図示の下記の情報を対応づけて登録するものである。

【００４３】

・コンテンツＩＤ：
・鍵　　：
・ユーザＩＤ　　：
・認証ＩＤ　　：
・その他　　：

ここで、コンテンツＩＤはユーザがダウンロードしたコンテンツＩＤであり、鍵は暗号化したコンテンツを復号する鍵であり、ユーザＩＤはコンテンツをダウンロードしたユーザＩＤであり、認証ＩＤはダウンロード要求したクライアントの固有の一意の認証ＩＤである。ここで、クライアントの固有の一意の認証ＩＤを対応づけて登録したことで、異なるクライアント（マシン）から同一ユーザＩＤが再ダウンロード要求しても異なる認証ＩＤであると判別し、再ダウンロードを不許可としたり、再課金したりするなどの処理が可能となる。

【００４４】図３の（ｃ）は、クライアント２側で管理するライセンステーブル３３の例を示す。このライセンステーブル３３は、図１のクライアント２側に用意し、図示の下記の情報を登録して管理するものである。

【００４５】

・コンテンツＩＤ：

・解読鍵　　：
・その他　　：
ここで、コンテンツＩＤは暗号化されたダウンロードを受けたコンテンツのＩＤであり、解読鍵はコンテンツを復号する鍵を認証ＩＤで暗号化したものである。このため、コンテンツ使用時には、ライセンステーブル３３中の解読鍵を、クライアント自身の認証ＩＤで復号して鍵を作成し、この作成した鍵でコンテンツＩＤで識別される暗号化されたコンテンツを復号し、復号した後のコンテンツを使用することで、許可された認証ＩＤのクライアント（マシン）でないと、暗号化されたコンテンツを復号して使用することができなく、暗号化したコンテンツの無断使用を防止することが可能となる。

【００４６】図４は、本発明の説明図を示す。これは、既述した図２のＳ７の不一致（ダウンロード要求したクライアント２の認証ＩＤと、図３の（ｂ）のコンテンツテーブル３２に登録されている認証ＩＤとが不一致、即ち、異なるクライアント（マシン）から同一ユーザＩＤ，同一コンテンツＩＤで再ダウンロード要求した場合）の詳細な動作説明である。

【００４７】図４の（ａ）は、フローチャート（その２）を示す。図４の（ａ）において、Ｓ３１は、メッセージ送信する。これは、既述した図２のＳ７の不一致の場合に、メッセージとして、図４の（ｂ）のメッセージをクライアント２に送信する。

【００４８】Ｓ３２は、処理選択・送信する。これは、Ｓ３１で送信されてきた、図４の（ｂ）のメッセージを表示し、図示の下記のいずれかを選択してサーバ１に送信（返答）する。

【００４９】・再課金してダウンロードする
・ダウンロードを中止する
Ｓ３３は、どの処理が選択されたか判別する。再課金承認の場合（図４の（ｂ）の再課金してダウンロードするが選択された場合）には、Ｓ３４で課金処理を行い、図２の（Ｃ）のＳ８に進む。一方、拒否の場合（図２の（ｂ）のダウンロード中止が選択された場合）には、ダウンロード処理を中止し、終了する。

【００５０】以上によって、クライアント１から
・ユーザＩＤ
・コンテンツＩＤ
・認証ＩＤ
を設定したダウンロード要求があり、このうちの、ユーザＩＤとコンテンツＩＤとが同一のエントリが図３のコンテンツテーブル３２に登録されており、認証ＩＤのみが異なり、異なるクライアント（マシン）２からの再ダウンロード要求と判明した場合に、問い合わせをクライアント２に行い、再課金承認のときは再課金処理して既述した図２のＳ８以降の処理で暗号化したコンテンツと、新たな認証ＩＤで暗号化した解読鍵をクライアント２に送信することが可能となる。

【００５１】図４の（ｂ）は、メッセージの例を示す。これは、既述した図４の（ａ）のＳ３１でサーバ１からクライアント２に送信するメッセージの例であり、ここでは、認証ＩＤのみがことなる再ダウンロード要求をサーバ１が受信したとき（既述した図２のＳ６のＮＧ）に、サーバ１が送信するメッセージの例であり、再ダウンロード時に、再課金を了承、あるいは再ダウンロードを中止のいずれかを選択するメッセージである。

【００５２】図５は、本発明の動作説明フローチャート（その３）を示す。これは、図２のＢに続いて行う処理である。図５において、Ｓ４１は、コンテンツ一覧の表示要求を行う。これは、図１のクライアント２を構成するＷｅｂブラウザ２１上に表示した例えばホームページの画面上でコンテンツ一覧を選択して要求する。

【００５３】Ｓ４２は、コンテンツ一覧を返信する。これは、Ｓ４１のコンテンツ一覧要求に対応して、Ｗｅｂサーバ１５がコンテンツ一覧を返信する。Ｓ４３は、コンテンツ表示・選択する。これは、Ｓ４２で返信されたコンテンツ一覧をＷｅｂブラウザ２１の画面上に表示し、ユーザがコンテンツ一覧からコンテンツを１つマウスなでクリックして選択する。

【００５４】Ｓ４４は、ユーザＩＤ（ＵＩＤ）を入力する。Ｓ４５は、認証ＩＤ（ＭＩＤ）を取得する。これらＳ４４、Ｓ４５はＷｅｂブラウザ２１がユーザＩＤを取り込むと共に、プラグイン２６を構成するソフトウエアに指示して認証ＩＤ（例えばハードディスク装置の番号）を取り込む。そして、これらユーザＩＤおよび認証ＩＤをＷｅｂサーバ１５に送信する。

【００５５】Ｓ４６は、ユーザＩＤをチェックする。これは、Ｓ４４で送信されてきたユーザＩＤが既述した図３の（ａ）のユーザ認証テーブル３１に登録されており、コンテンツをダウンロードする資格があるかチェックする。この際、合わせてユーザのパスーワードも一致するかチェックする。チェックした結果、ＯＫとなった場合には、Ｓ４７に進む。ＮＧの場合には、エラー処理を行う。

【００５６】Ｓ４７は、コンテンツテーブル中に同じユーザＩＤがあるか判別する。ＹＥＳの場合には、Ｓ４８に進む。ＮＯの場合には、図２のＳ８に進む。Ｓ４８は、コンテンツテーブル中の同じユーザＩＤに対応する認証ＩＤが一致するか判別する。これは、今回のダウンロード要求のあったときの認証ＩＤが、コンテンツテーブル３２中のユーザＩＤとコンテンツＩＤとが一致するエントリ中の認証ＩＤ（過去にダウンロードを受けたときの認証ＩＤ）と一致するか判別する。ＹＥＳの場合には、図２のＳ８に進む。ＮＯの場合には、Ｓ４９でコンテンツテーブル中の認証ＩＤと鍵で解読鍵を作成し、図２のＳ９に進む。

【００５７】以上によって、ダウンロード要求を受信したサーバ１では、ユーザＩＤ、コンテンツＩＤが一致す

るエントリがコンテンツテーブル３２から見つかったが、認証ＩＤのみが異なる場合（同一ユーザＩＤから同一コンテンツＩＤのダウンロード要求があり、異なるクライアント（マシン）からのダウンロード要求であった場合）には、Ｓ４９でここでは、コンテンツテーブル３２中の認証ＩＤと鍵（暗号化したコンテンツを復号する鍵）で暗号化した解読鍵を作成し、この解読鍵と暗号化したコンテンツとを一緒にしてクライアント２に送信する。これにより、異なるマシン（クライアント）から以前にダウンロードしたコンテンツを同一ユーザが再ダウンロード（以前のダウンロードに失敗し、他のマシン（正常に動作するマシン）から再ダウンロード）することなどが可能となる。

【００５８】図６は、本発明の動作説明フローチャート（その４）を示す。これは、図２のＢに続いて行う他の処理である。ここで、Ｓ５１からＳ５８は、図５のＳ４１からＳ４８と同一であるので、説明を省略する。

【００５９】図６において、Ｓ５９は、Ｓ５８でダウンロード要求したユーザＩＤ、コンテンツＩＤ、認証ＩＤのうちの、認証ＩＤのみが異なるエントリがコンテンツテーブル３２に登録されていたので、コンテンツテーブル３２に登録されている同じユーザＩＤのコンテンツに対して現在の認証ＩＤによって解読鍵を作成する。これにより、以前にダウンロードしたコンテンツについて、現在の認証ＩＤで暗号化した解読鍵が作成されることとなる。

【００６０】Ｓ６０は、現在のダウンロード要求のコンテンツに対しても現在の認証ＩＤによって解読鍵を作成する。これにより、現在ダウンロードしようとする同じコンテンツＩＤのコンテンツ（例えば改良されたコンテンツ）について、現在の認証ＩＤで暗号化した解読鍵が作成されることとなる。

【００６１】Ｓ６１は、暗号化したコンテンツと解読鍵をクライアント２に送信する。そして、図２のＳ１１に進む。以上によって、ダウンロード要求を受信したサーバ１では、ユーザＩＤ、コンテンツＩＤが一致するエントリがコンテンツテーブル３２から見つかったが、認証ＩＤのみが異なる場合（同一ユーザＩＤから同一コンテンツＩＤのダウンロード要求があり、異なるクライアント（マシン）からのダウンロード要求であった場合）には、

・Ｓ５９でコンテンツテーブル３２に登録されているコンテンツ（以前にダウンロードした古いコンテンツ）に対して現在の認証ＩＤで解読鍵を作成し、

・Ｓ６０で現在のダウンロード要求したコンテンツ（現在の最新のコンテンツ）に対して現在の認証ＩＤで解読鍵を作成し、

両者のコンテンツと解読鍵をそれぞれクライアントに送信する。これにより、異なるマシン（クライアント）から以前にダウンロードした古いコンテンツを同一ユーザが再ダウンロード、および同一コンテンツＩＤの現在の最新のコンテンツをダウンロードすることが可能となる。

【００６２】

【発明の効果】以上説明したように、本発明によれば、同一ユーザによる異なるクライアント（端末）２からの再ダウンロード要求に対して不許可あるいは再課金などして再ダウンロードする構成を採用しているため、コンテンツの無断使用を防止すると共にコンテンツの適切な使用を実現できる。

【図面の簡単な説明】

【図１】本発明のシステム構成図である。

【図２】本発明の動作説明フローチャート（その１）である。

【図３】本発明のテーブル例である。

【図４】本発明の説明図である。

【図５】本発明の動作説明フローチャート（その３）である。

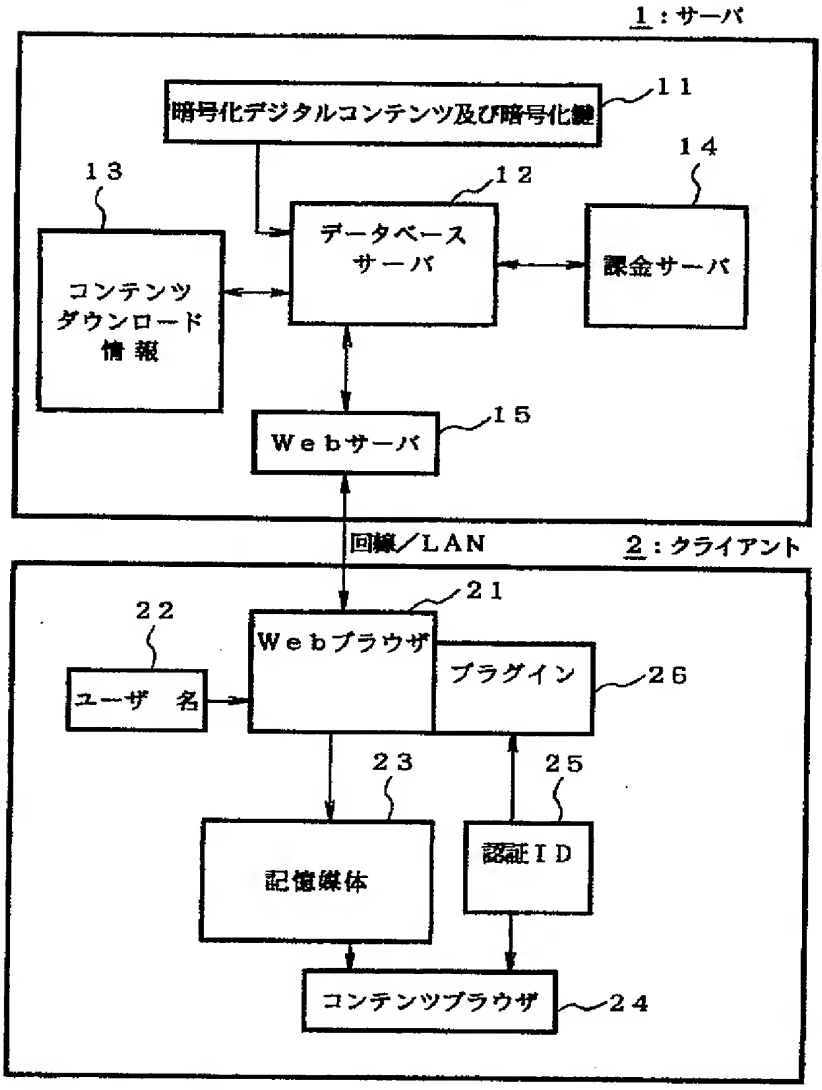
【図６】本発明の動作説明フローチャート（その４）である。

【符号の説明】

１：サーバ
１１：暗号化デジタルコンテンツ及び暗号化鍵
１２：データベース
１３：コンテンツダウンロード情報
１４：課金サーバ
１５：Ｗｅｂサーバ
２：クライアント（端末）
２１：Ｗｅｂブラウザ
２３：記憶媒体
２４：コンテンツブラウザ
２５：認証ＩＤ
２６：プラグイン

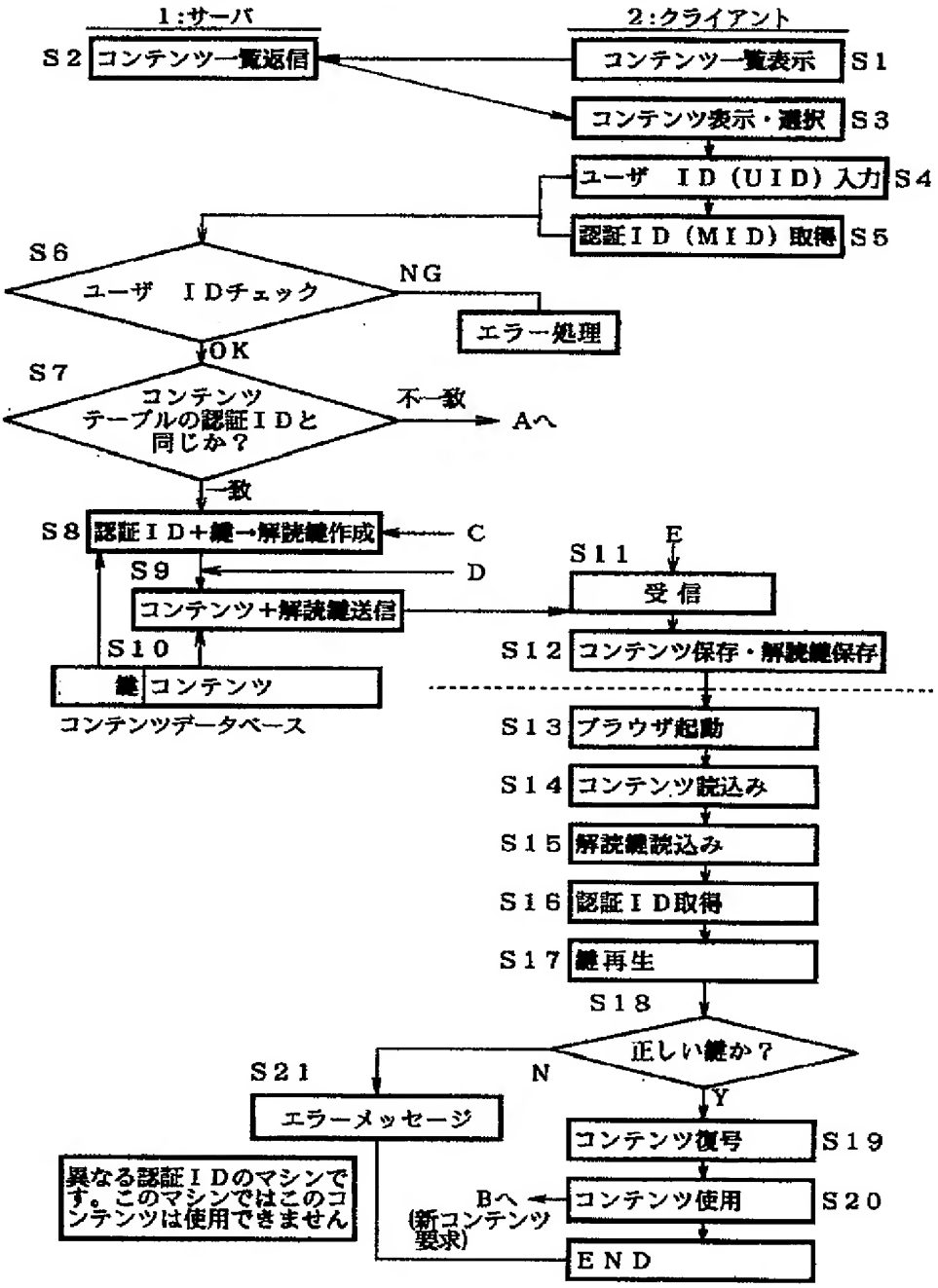
【図１】

本発明のシステム構成図



【図２】

本発明の動作説明フローチャート（その１）



【図３】

本発明のテーブル例

(a) サーバ：ユーザ 認証テーブル

ユーザ ID	パスワード
USER001	PASSAAA
USER002	PASSQQQ

(b) サーバ：コンテンツテーブル

コンテンツID	鍵	ユーザ ID	認証ID
CID0001	123456	USER001	1111
CID0002	XYZ001	USER998	ABCD

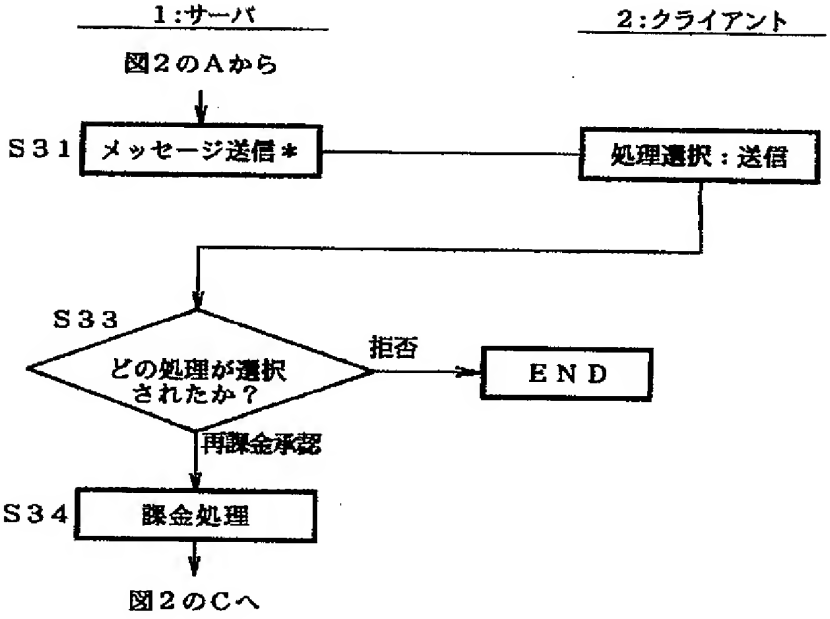
(c) クライアント：ライセンステーブル

コンテンツID	解読鍵
CID0001	654321
CID1234	AABBCC

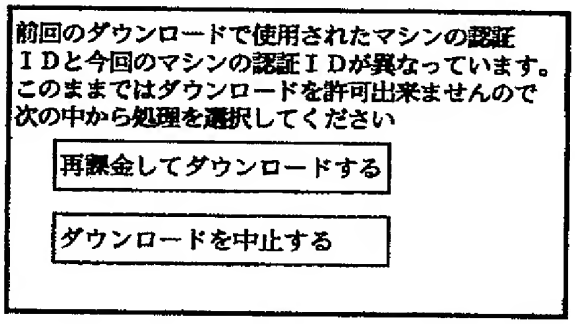
【図４】

本発明の説明図

（ａ）フローチャート（その２）

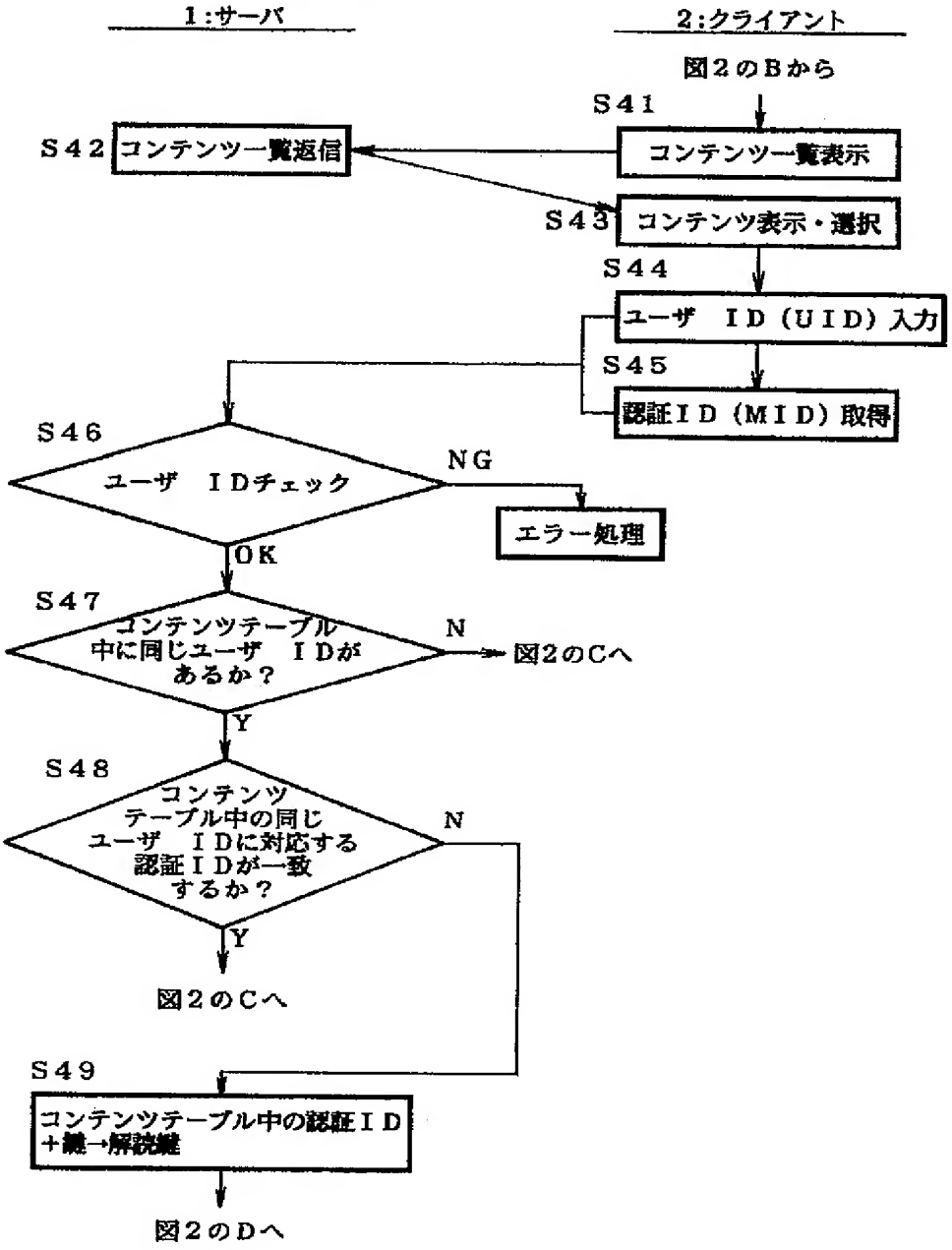


（ｂ）メッセージ



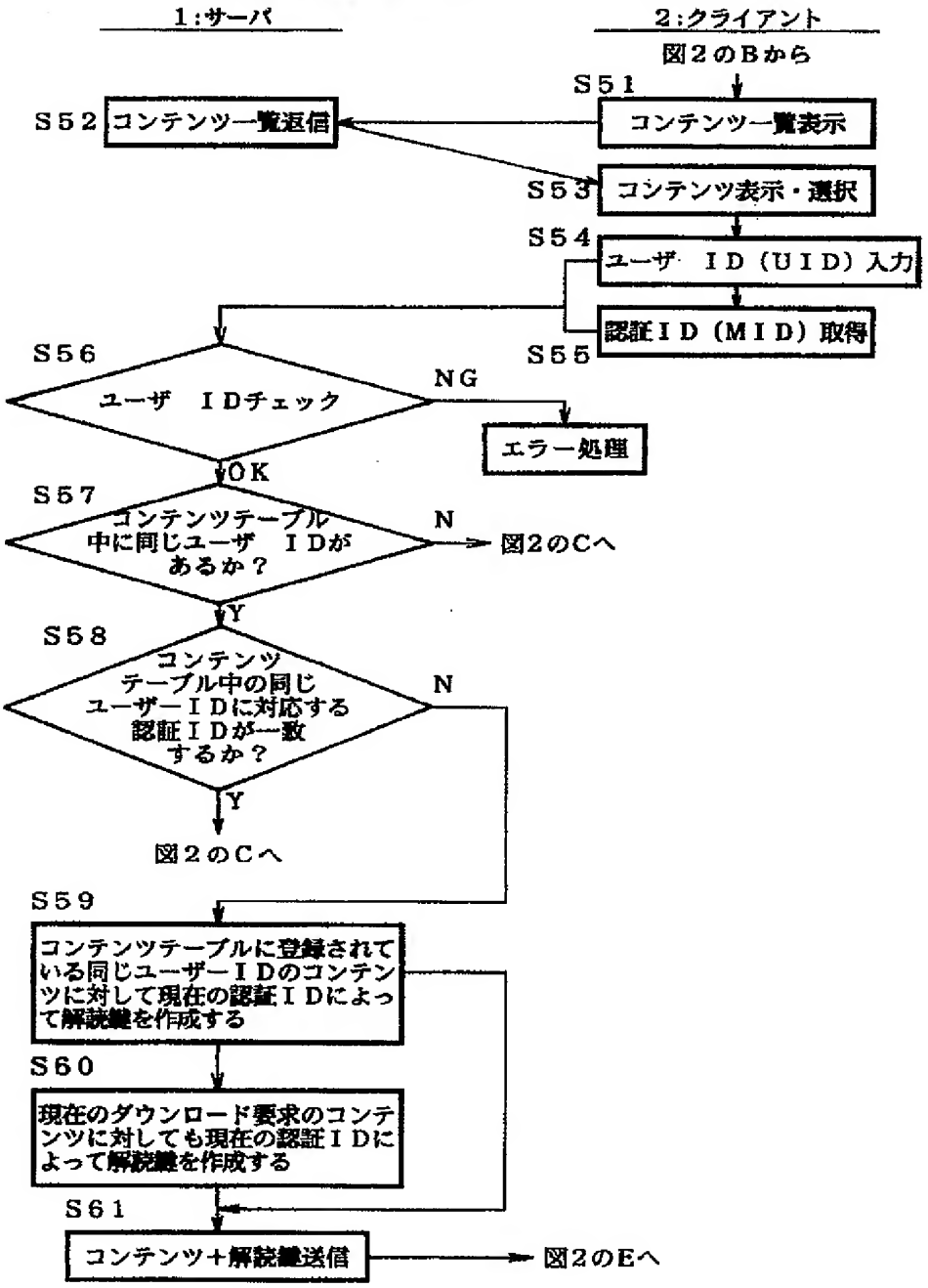
【図５】

本発明の動作説明フローチャート（その３）



【図６】

本発明の動作説明フローチャート（その４）



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ 17/60		Ｇ０６Ｆ 15/21	Ｚ
			３３０

Ｆターム(参考) 5B017 AA06 AA07 BA05 BA07 BB02
BB10 CA09 CA15 CA16
5B049 AA05 BB11 BB60 CC10 EE23
GG04 GG10
5B076 AB10 FA01 FA16 FA20 FB05
FB07 FC10
5B085 AC04 AE02 AE04 AE13
5B089 GA11 GA21 GB04 HA01 HA06
JA08 JA22 JA33 JB04 JB05
KA15 KA17 KB06 KB12 KC58
KH30 LB15

Japanese Patent Application Laid-Open No. 2000-242604
(P2000-242604A)
Published
September 8, 2000
(21) Application No. Patent Application No. 11-42197
(22) Filing Date February 19, 1999
(71) Fujitsu, Ltd.
(72) Takahiro Haraki

(54) [Title of the Invention] Contents distribution system, terminal device and recording medium

(57) [Abstract]
[Problem] The present invention relates to a contents distribution system, a terminal device and a recording medium and is intended to prevent contents from being used without permission and realize appropriate use of contents by giving a nonpermission or recharging to a re-download request by the same user from a different terminal device.
[Means for Solving] A system is adapted to include a unit that receives a user ID, a unique authentication ID for a terminal, and a content download request; a that records the user ID, the authentication ID and a transmitted content in relation; a unit that generates a decryption key from the authentication ID and a key of the content when the received user ID and content are recorded in the table and when the received ID is identical with the recorded ID, or when a user ID and a content are not recorded in the table, records the user ID, an authentication ID, and the content in relation and generates a decryption key from the authentication ID and the key of the content; and a unit that transmits the generated decryption key and the coded content to the terminal.

[Scope of Claim]
[Claim 1] A system for distributing a content, comprising a unit that receives a user ID, a unique authentication

ID for a terminal, and a content download request;

a table that records the user ID, the authentication ID and a transmitted content in relation;

a unit that generates a decryption key from the authentication ID and a key of the content when the received user ID and content are recorded in the table and when the received ID is identical with the recorded ID, or when a user ID and a content are not recorded in the table, records the user ID, an authentication ID, and the content in relation and generates a decryption key from the authentication ID and the key of the content; and

a unit that transmits the generated decryption key and the coded content to the terminal.

[Claim 2] The system for distributing a content according to claim 1, wherein when the received user ID and the content are recorded in the table and the received authentication ID is not identical with the recorded authentication ID, the system transmits a notice that the terminal is recharged and when a response that the recharging is consented to, generates a decryption key from the authentication ID and the key of the content, and then transmits the generated decryption key and coded content to the terminal.

[Claim 3] The system for distributing a content according to claim 1, wherein when the received user ID and content are recorded in the table and the received authentication ID is different from the recorded authentication ID, the system performs recharging, generates a decryption key from the authentication ID and the key of the content, and transmits the generated key and the content coded with the key to the terminal.

[Claim 4] The system for distributing a content according to claim 1, wherein when the received user ID and the content are recorded in the table, and when the received authentication ID is different from the recorded authentication ID, the system generates a first decryption key from the received authentication ID and the key of the content recorded in the table and a second decryption key from the received

authentication key and the key of the current content of which a download request has been made, and transmits the generated first decryption key together with the coded content, and the generated second decryption key with the coded content to the terminal.

[Claim 5] A terminal device comprising:

a unit that transmits a user ID, a unique authentication ID of the terminal device itself, and a content download request;

a unit that receives the transmitted decryption key and content;

a unit that generates a key of the content for the received decryption key based on a predetermined authentication ID of the terminal device itself;

a unit that decodes the received coded content based on the generated key; and

a unit that uses the decoded content.

[Claim 6] The terminal device according to claim 5, wherein the unique authentication ID of the terminal is a unique number of predetermined hardware of the terminal.

[Claim 7] A computer readable recording medium having recorded therein a program that causes a computer to operate as:

a unit that receives a user ID, a unique authentication ID for a terminal, and a content download request;

a table that records the user ID, the authentication ID and a transmitted content in relation;

a unit that generates a decryption key from the authentication ID and a key of the content when the received user ID and content are recorded in the table and when the received ID is identical with the recorded ID, or when a user ID and a content are not recorded in the table, records the user ID, an authentication ID, and the content in relation and generates a decryption key from the authentication ID and the key of the content; and

a unit that transmits the generated decryption key and

the coded content to the terminal.

[Detailed Description of the Invention]

[0001]

[Technical Field to Which the Invention Belongs] The present invention relates to a content distribution system that distributes and uses a distributed content, a terminal device, and a recording medium.

[0002]

[Prior Art] In recent years, digital contents, such as music, motion picture, and further programs of TV games can be purchased on-line in addition to purchasing in the shop along with popularization of communication. In particular, emergence of a WWW server in the Internet allows users to connect with the WWW server, download a list of contents, displays a content on a screen, visually confirm the content, and select and purchase the content.

[0003] From the nature of a digital content, the content is not deteriorated when it is copied. This allows endless copying, so that the right of the author of the content can not be protected. Accordingly, it is demanded to prevent others from using without permission a content which a user duly purchased through the Internet or the like network.

[0004]

[Problem(s) to be Solved by the Invention] For this reason, for example, when a user intends to duly purchase a content from a WWW server through the network, download and store the content in a hard disk device and use it, problem may occur if download of the content fails due to some troubles and downloading is again attempted. That is, if the WWW server stores the user ID of the user who duly purchased the content and re-downloading is permitted when the user ID with which a re-download request is made is stored, then, re-downloading is permitted when a re-download request is made with designating the user ID from another personal computer. If the user ID is stolen, the contents will be unrighteously downloaded from the

WWW server to a third party. Therefore, it is demanded to prevent use of contents without permission and give a permission to appropriate use when a re-download request is made.

[0005] To solve these problems, it is an object of the present invention to reject or recharge when a re-download request from a different terminal by the same user is made to prevent use of a content without permission and on the other hand realize appropriate use of the content.

[0006]

[Means for Solving the Problem(s)] Referring to Fig. 1, the means for solving the problems is described. In Fig. 1, a server 1 receives a user ID, a unique authentication ID for a terminal device and a request for download of a content, generates a decryption key from the authentication ID and a key of the contents, and transmits the generated decryption key and coded content to a terminal.

[007] A client 2 transmits a user ID, a unique authentication ID of its own, and a quest for downloading a content, receives a transmitted decryption key and content, generates a key of content relative to the received decryption key based on the predetermined authentication ID of its own, and decodes the coded content based on the generated key.

[0008] Next, its operation is described.

When the server 1 receives a user ID, a unique authentication ID of a terminal, and a re-download request a content, he received user ID and the content are recorded in a contents table, and the received authentication is identical with the recorded authentication ID, a decryption key is generated from the authentication ID and the key of the content, or when a user ID and a content are not recorded in the table, the server 1 records the user ID, an authentication ID, and the content in relation and generates a decryption key from the authentication ID and the key of the content, and transmits the generated decryption key and coded content to the terminal.

[0009] When the received user ID and content are recorded in the contents table and the received authentication ID were

not identical, a notice of recharging is transmitted to the terminal. When a response from the terminal to consent is received, a decryption key is generated from the authentication ID and the key of the content, and the generated decryption key and the coded content are transmitted to the terminal.

[0010] When the received user ID and the content are recorded in the contents table and the received authentication ID is different from the recorded authentication ID, recharging is performed, a decryption key is generated from the authentication ID and the key of the content, and the generated decryption key and the coded content are transmitted to the terminal.

[0011] When the received user ID and the content are recorded in the contents table and the received authentication ID is different from the recorded authentication ID, a first decryption key is generated from the received authentication ID and the key of the content recorded in the contents table. A second decryption key is generated from the received authentication ID and the key of the current content of which a download request has been made. The generated first decryption key and coded content as well as generated second decryption key and coded content are transmitted to the terminal.

[0012] A client (terminal 2) transmits the user ID, unique authentication ID of its own, and a content download request, receives a transmitted decryption key and a content, generates a key of the content relative to the received decryption key, decodes the coded contents received based on the predetermined authentication ID of its own, and use the decoded content.

[0013] The unique authentication ID of the client (terminal) 2 is used as a unique number of predetermined hardware. Therefore, a re-download request from a different client (terminal) 2 by the same user is given nonpermission or recharged, thereby preventing the content from being used without permission and appropriate use of the content can be realized.

[0014]

[Embodiment] Next, referring to Figs. 1 to 6, an embodiment and operation of the present invention will be sequentially described in detail.

[0015] Fig. 1 is a diagram illustrating system architecture of the present invention. In Fig. 1, a server 1 distributes (downloads) a digital content to a plurality of clients 2. Here, the server 1 is constituted by, e.g., 11 to 15 illustrated.

[0016] A coded digital content and coded key 11 includes a coded digital content distributed to users and its coded key (a decryption key for coding a digital content or decoding the coded digital content), which are stored in a database.

[0017] A database server 12 is a server that manages the database in which the coded digital content and an encryption key 11. Here, the database server 12 reads out the content of which a download request has been made from a user and its key (decryption key) and transfers them to a Web server 15. The database serve 12 also notifies the downloaded content and user ID to charging server 14 and perform charging.

[0018] A content download information 13 is stored content download information is information of download of which a request has been made from the user and is intended to manage contents downloaded by a user based on the user authentication table and the content table in Fig. 3(a) and (b) described hereinafter.

[0019] The charging server 14 manages user by user usage fees for contents downloaded by users, and counts every predetermined period and debit each user. Web server 15 is connected by the client 2 or a communication line or LAN and transmits a list of contents, receive requests for downloading contents selected from the list of contents, and downloads the requested content.

[0020] The client 2 may be a terminal (personal computer) used by a user and is connected to the Web server 15 through a communication line or LAN and download and display the list

of contents. The client 2 requests downloading the selected contents on the displayed list of contents, stores the downloaded contents in a memory medium 23, and decodes the content coded with a key. The client 2 is constituted by 21 to 26.

[0021] A web browser 21 is connected to Web server 15 through a communication line or LAN, and selects and displays the list of contents. A user name 22 is a name (full name of user, user ID and the like information) of a user who uses a content (use a content by audition or display of a content).

[0022] A recording medium 23 is a recording medium that stores a content downloaded from the Web server 15, and includes, for example, a hard disk device and DVD-RAM.

[0023] A content browser 24 uses coded contents stored in the storage medium 23 after decoding it based on a unique authentication ID that the hardware of the client 2 has (for example, number of the hard disk device) 25 and a decryption key (the decryption key downloaded together from the Web server 15 when the content is down loaded, see Fig. 2).

[0024] An authentication ID 25 is a unique ID to the client (terminal) 2, and is, for example, the number of the hard disk device, which is hardware. A plug-in 26 is software that has various functions to be incorporated into the Web browser 21. Here, the Web browser 21 takes unique authentication ID 26 from the hardware of the client (terminal) 2 and transmits the authentication ID 26 together with the content request to the Web server 15 (see, for example, Fig. 2).

[0025] Next, in the order of the flowchart in Fig. 2, the operation of the architecture of Fig. 1 is described in detail. Fig. 2 is a flowchart (No. 1) illustrating the operation of the present invention. Here, a server 1 and a client 2 correspond to the server 1 and the client 2 in Fig. 1.

[0026] In Fig. 2, S1 performs request for display of the list of contents. This is done by selecting the list of contents on a screen of, for example, a homepage displayed on the Web browser 21 constituting the client 2 in Fig. 1.

[0027] S2 returns a contents list. The Web server 15 returns the contents list to in response to the request for contents list by S1. S3 displays and selects a content. This is done by displaying the contents list on the screen of the Web browser 21 and selecting a content from the contents list with a click by a mouse or the like.

[0028] S4 inputs user ID (UID).S5 obtains authentication ID (MID). In S4 and S5, the Web browser 21 takes user ID in and gives instruction to software that constitutes the plug-in 26 to take the authentication ID (for example, the number of hard disk device) in. Then, the user ID and authentication ID are transmitted to the Web server 15.

[0029] S6 checks the user ID. The user ID transmitted by S4 is recorded in the user authentication table 31 in Fig. 3(a) described layer and checks whether to be qualified to download a content. On this occasion, whether or not the password coincides is also checked. The result of the check indicates OK, the operation proceeds to S7. In the case of NG, error treatment is performed.

[0030] S7 determines whether to be identical with the authentication ID in the contents table. This is done by referring to the contents table 32 in Fig. 3(b) and determine whether an entry exists that is identical with the user ID and content ID of which requests for downloading are made in S4 and S5 and whether the authentication ID transmitted this time is identical to the authentication ID in the entry. When these coincide, then there is an entry in the contents table 32 in Fig. 3(b) in which all the three:

- Content ID
- User ID
- Authentication ID

of which download request has been made coincide, and it reveals that the same personal computer (client 2) has downloaded, so that s second (or subsequent) download to a user to whom a license of use has already been given (for example, during the downloading, download failed for some reason or another and this

is a request for second re-downloading), so that the operation proceeds to S8. Although not shown, when among

- Content ID
- User ID
- Authentication ID

of which download request has been made this time, the user ID and the content ID are not set in the contents table 32 in Fig. 3(b), it reveals that the user has for the first time requested download of the content. Accordingly, as an initial treatment, content ID, user ID, and authentication ID are set in the contents table 32. Thereafter, the operation proceeds to S8.

[0031] S8 makes a decryption key based on the authentication ID + the key. That is, a decryption key is made based on the authentication ID received from the client 2 and the key of the content of which download request has been made (for example, the authentication ID is coded with a key to make a decryption key..

[0032] S9 transmits content + decryption key. This results in that the server 1 has successfully transmitted a coded content and the decryption key made in S8 to the client 2.

[0033] S10 shows an example of a contents database. Here is shown a manner in which a content is constituted by the coded content and the key. The key of the content is treated as the key in S8 already described and the authentication ID is coded with the key to make a decryption key.

[0034] In S11, the client 2 receives a coded content and a decryption key, transmitted from the server 2 in S9. S12 stores the content and decryption key.

[0035] S13 starts a browser. That is, the content browser 24 in Fig. 1 is started. S14 reads the content.

[0036] S15 reads the decryption key. In S14 and S15, the coded content stored in S12 and the decryption key are read by the content browser 24. S16 obtains an authentication ID. That is, the content browser 24 unique number specific to the predetermined hardware in the client (personal computer, etc.)

2 is obtained as a unique number of a hard disk device as an authentication ID.

[0037] S17 regenerates a key. That is, the decryption key read out and obtained in S14 to S16 is decoded by the authentication ID to regenerate a key (a key to decode the coded content).

[0038] S18 determines whether the key is authentic or not. In the case of YES, the operation proceeds to S19. In the case of NO, an error message is displayed in S21. For example, as illustrated in the drawing, a message is displayed:

"・Your machine is with a different authentication ID. This content is not usable with this machine!" and the operation is ended.

[0039] S19 decodes the content. That is, the downloaded coded content is decoded with a key to convert the original content. S20 uses a content. That is, the content decoded in S19 is used. For example, in the case of music, the content is auditioned, in the case of a program of TV game, the program is operated and the TV game is played. Various kinds of useful information, such information is read, used, etc. to perform a work.

[0040] As mentioned above, the client 2tansmits the content ID, user ID, and authentication ID to the server 1, the server 1 makes a decryption key from the authentication ID and the key, and transmits together with the coded content to the client 2. The client 2 that receives the decryption key and coded content decodes a key from the decryption key based on the authentication ID unique to the client 2 itself, decodes the coded content with a decoded key, to generate the original content and use the generated content. This results in that even the same user can not decode the coded content with a different client (different machine), so that use without permission can be prevented and at the same time re-downloading is allowed with the same client (the same machine) to decode the content and use it.

[0041] Fig. 3 illustrates an example of the table of the

present invention. Fig 3(a) shows an example of user authentication tale 31 managed by the server 1 side. The user authentication table 31 is provided on the side of the server 1 in Fig. 1 and user ID of subject who is permitted use of the content and charged and password are related to each other and recorded in advance. By providing the user authentication table 31 and referred to in S6 in Fig.2 to confirm user ID and password, and when these are recorded, it is determined OK (user authentication is OK).

[0042] Fig. 3(b) shows an example of the contents table 32 managed on the server 1 side. The contents table 32 is provided on the server 1 in Fig. 1 and the following information illustrated in Fig. 3(b) in relation to each other.

[0043]

- Content ID
- Key
- User ID
- Authentication ID
- Others

Here, the content ID is one downloaded by the user, the key decodes the coded content, user ID is a user ID that downloaded the content, the authentication ID is a unique authentication ID specific to the client of which download request is made. Here, recording the unique authentication ID related to each other enables a treatment such that when the same user ID requests re-downloading from a different client (machine), this is determined to be with a different authentication ID and a treatment such as non-permission of re-downloading or recharging is made possible.

[0044] Fig. 3(c) shows an example of a license table 33 managed on the side of the client 2. The license table 33 is provided on the side of the client 2 in Fig. 1 and the following information shown in the drawings are recorded and managed.

[0045]

- Content ID:
- Decryption key

・ Others

Here, the content ID is an ID of the content that was subject to coded download. The decryption key is a key that decodes a content coded with an authentication ID. For this reason, when the content is used, the decryption key in the license table 33 is decoded with the authentication ID of the client itself to make a key. The coded content distinguished by the content ID is decoded with the key thus made and the content after decoding is used. With this, other clients (machines) than the client (machine) with the permitted authentication ID can not decode the coded content and use it, so that use of the coded content without permission can be prevented.

[0046] Fig. 4 is a diagrammatic illustration of the present invention. This is detailed description of operation in the case of discrepancy in S7 in Fig. 2 as already described (the authentication ID of the client 2 that issues a download request and the authentication ID recorded in the contents table 32 in Fig. 3(b) is in disagreement with each other, that is, download request is made with the same user ID and the same content ID from a different client (machine).

[0047] Fig. 4(a) is a flowchart (No. 2). In Fig. 4(a), S31 transmits a message. That is, in the case of disagreement of S7 in Fig. 2 already described, the message in Fig. 4(b) is transmitted to the client 2.

[0048] S32 selects treatment and transmits. That is, the message in Fig. 4(b) transmitted in S31 is displayed and any one of the following illustrated cases is selected and transmitted (responded) to the server 1.

[0049] ・Recharge and download

・Discontinue

S33 determines which treatment is selected. In the case where recharging is accepted (Recharge and download in Fig. 4(b) is selected), charging treatment is performed in S34 and the operation proceeds to S8 in Fig. 2(C). On the other hand, in the case of refusal (the case where discontinue download in Fig. 2(b) is selected), the download treatment is discontinued and

terminated.

[0050] From the above, when a download request with setting

- User ID
- Content ID
- Authentication ID

is made from the client 1, and an entry in which user ID and content ID are the same is recorded in the contents table 32. When this is proved to be a re-download request from a different client (machine), an inquiry is sent to the client 2 and in the case where a response is that recharging is accepted, recharging treatment is performed and the coded content and a decryption key coded with a new authentication ID can be transmitted to the client 2.

[0051] Fig. 4(b) illustrates an example of message. This is an example of message transmitted from the server 1 to the client 2. Here, when the server 1 receives re-download request with only authentication ID being different (NG in S6 in Fig. 2 already described). That is, a message asking to select either one of accepting recharging or discontinuing re-downloading at the time of re-downloading.

[0052] Fig. 5 is a flowchart illustrating the operation of the present invention. This is a treatment performed subsequent to B in Fig. 2. In Fig. 5, S41 requests display of the contents list. This request is made by selecting the contents list on a screen of, for example, a homepage displayed on the Web browser 21 that constitutes the client 2 in Fig. 1.

[0053] S42 returns the contents list. That is, in response to the request for the contents list in S41, the Web server 15 returns the contents list. S43 displays and selects the contents list. That is, the contents list returned in S42 is displayed on a screen of the Web browser 21 and the user selects a content from the contents list by clicking by a mouse or the like.

[0054] S44 inputs a user ID (UID). S45 obtains authentication ID (MID). In S44 and S45, the Web browser 21 takes user ID in and gives instruction to software that

constitutes the plug-in 26 to take the authentication ID (for example, the number of hard disk device) in. Then, the user ID and authentication ID are transmitted to the Web server 15.

[0055] S46 checks the user ID. The user ID transmitted by S44 is recorded in the user authentication table 31 in Fig. 3(a) described layer and checks whether to be qualified to download a content. On this occasion, whether or not the password coincides is also checked. The result of the check indicates OK, the operation proceeds to S47. In the case of NG, error treatment is performed.

[0056] S47 determines whether or not user ID is identical with the authentication ID in the contents table. If YES, the operation proceeds to S48. If NO, the operation proceeds to S8 in Fig. 2. S48 determines whether or not the corresponding authentication ID coincides with each other for the same user ID. That is, determination is made whether or not the authentication ID when download request is made this time is identical to the authentication ID in an entry where the user ID is identical to the content ID in the contents table 32. If YES, the operation proceeds to S8 in Fig. 2, and if NO, a decryption key is made from the authentication ID in the contents table and a key in S49 and the operation proceeds to S9 in Fog. 2.

[0057] As mentioned above, the server 1 that received a download request, an entry in which the user ID and the content ID are identical to each other is found in the contents table 32. However, when the authentication ID alone is different (a download request for identical content ID from the identical user ID is made and this is a download request from a different client (machine), in S49 here a coded decryption key is made from the authentication ID and a key (a key to decode the coded content) in the contents table 32, and the decryption key together with the coded content is transmitted to the client 2. This enables the same user to re-download the content that is previously downloaded through a different machine (client)(previous downloading was unsuccessful and

re-downloading from another machine (operating normally).

[0058] Fig. 6 is a flowchart (No. 4) illustrating the operation of the present invention. This is other treatment to be performed subsequently to B in Fig. 2. Here, S51 to S58 are identical with S41 to S48 in Fig. 5, description thereof will be omitted.

[0059] In Fig. 6, since among the user ID, content ID, and authentication ID of which download is requested in S58, an entry in which only the authentication ID is different is recorded in the contents table 32, S59 makes a decryption key with current authentication ID to the content with the same user ID recorded in the contents table 32. This enables make a coded decryption key with the current authentication ID for the previously down loaded content.

[0060] S60 makes a decryption key with the current authentication ID for a current download request. This enables a decryption key coded with current authentication Id to be made for a content with the same content ID (for example, improved content) of which downloading is currently intended.

[0061] S61 transmits a coded content and a decryption key to the client 2. Then the operation proceeds to S11 in Fig. 2. By the foregoing, in the server 1 that receives a download request, an entry in which the user ID and the content ID are identical has been found. However, in the case where only the authentication ID is different (in the case where a download request is made from the same user ID with the same content ID but this is a download request from a different client (machine)),

- For the content recorded in the contents table 32 in S59 (previously downloaded old content), a decryption key is made with the current authentication ID,
- For content currently download is requested in S60 (currently the newest content), a decryption key is made with current authentication ID,

and both the contents and decryption keys are each transmitted to the client. This enables the old content previously

downloaded from different machine (client) to be re-downloaded by the same user and currently the newest content with the same content ID to be downloaded.

[0062]

[Effects of the Invention] As described above, according to the present invention, re-download request by the same user from the different client (terminal) 2 is not permitted or recharged for re-downloading, use of content without permission can be prevented and at the same time appropriate use of the content can be realized.

[Brief Description of the Drawings]

[Fig. 1] Fig. 1 is a diagram illustrating a system architecture of the present invention.

[Fig. 2] Fig. 2 is a flowchart (No. 1) for illustrating the operation of the present invention.

[Fig. 3] Fig. 3 is an example of a table used in the present invention.

[Fig. 4] Fig. 4 is a diagram illustrating the present invention.

[Fig. 5] Fig. 5 is a flowchart (No.3) illustrating the operation of the present invention.

[Fig. 6] Fig. 6 is a flowchart (No.4) illustrating the operation of the present invention.

[Description of Symbols]

1: Server
11: Coded digital content and coded key
12: Database
13: Content download information
14: Charging server
15: Web server
21: Client (terminal)
23: Storage medium
24: Content browser
25: Authentication ID
26: Plug-in

[Fig. 1]

Diagram of system architecture of the present invention

1: Server
11: Coded digital content and coded key
12: Database server
13: Content download information
14: Charging server
15: Web server
2: Client Communication/LAN
21: Web browser
22: User name
23: Storage medium
24: Content browser
25: Authentication ID
26: Plug-in

[Fig. 2]
Flowchart (No. 1) illustrating operation of the present invention
1: Server
2: Client
S1: Contents list display
S2: Contents list return
S3: Contents display/selection
S4: User ID (UID) input
S5: Authentication ID (MID) Obtention
S6: User ID Check Error treatment
S7: Same with authentication ID in contents table?
S8: Authentication ID + Key Decryption key making
S9: Content + Decryption key transmission
S10: Key|Content
Content database
S11: Reception
S12: Content storage Decryption key storage
S13: Browser Start
S14: Content reading
S15: Decryption key reading
S16: Authentication ID obtention

S17: Key regeneration
S18: Is correct key?
S19: Content decoding
S20: Content use To B (new content request)
S21: Error message
Your machine is with different authentication ID. This content is not usable with this machine!

[Fig. 3]
An example of table of the present invention
(a) Server: user Authentication table
User ID Password

(b) Server : content table
Content ID Key User ID Authentication ID
(c) Client : License table

[Fig. 4]
Diagrammatical illustration of the present invention

(a) Flowchart (No. 2)

1: Server 2: Client

From Fig. 2A

S31: Message transmission
Treatment Selection: Transmission

S33: Which treatment is selected? Refusal
Re-charging accepted

S34: Charging treatment
To Fig. 2C

(b) Message
Authentication ID used in previous download and authentication ID of the machine are different. Download is not permitted if this state continues. Select one of treatments below:

Recharge and download

Discontinue download

[Fig. 5]
Flowchart illustrating operation of the present invention (No. 3)
1: Server 2: Client
From Fig. 2 B
S41: Contents list display
S42: Contents list return
S43: Contents list display/selection
S44: User ID (UID) input
S45: Authentication ID (MID) obtention
S46: User ID Check
Error treatment
S47: Is same user ID in content table?
S48: Do authentication IDs coincide corresponding to same user IDs in contents table?
To Fig. 2 C
S49: Authentication ID + Key →Decryption key
To Fig. 2 D

[Fig. 6]
Flowchart illustrating operation of the present invention (No. 4)
1: Server 2: Client
S51: Contents list display
S52: Contents list return
S53: Contents list display/selection

S54: User ID (UID) input

S55: Authentication ID (MID) obtention

S56: User ID Check

Error treatment

S57: Is same user ID in content table?

S58: Do authentication IDs coincide corresponding to same user IDs in contents table?

To Fig. 2 C

S59: Makes a decryption key with current authentication ID to the content with the same user ID recorded in the contents table.

S60: Makes a decryption key with the current authentication ID for a current download request.

S61: Content + Decryption key transmission To Fig. 2 E